Auftragsverarbeitungsvertrag gemäß
Artikel 28 Absatz 3 Europäischen Datenschutz-Grundverordnung
(DS-GVO)

zum Hauptvertrag: _____

Zwischen

der Technischen Universität Dresden,
Mommsenstr. 11, 01069
vertreten durch den Kanzler

– Verantwortlicher –

und

Kontaktdaten
vertreten durch den*die Vertretungsberechtigte*n …

– Auftragsverarbeiter –

ERLÄUTERUNGEN:

- Der vorliegende Vertragstext basiert auf dem Durchführungsbeschluss (EU) der Kommission vom 4. Juni 2021 (EU) Nr. 2021/915 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates (ABl. 199/18 vom 07.06.21).

- Die oben genannten und im folgenden aufgeführten Standardvertragsklauseln sind mit einer Klausel 11 (Abschnitt IV) sowie in den Anhängen um zusätzliche Regelungen ergänzt. Diese sind in roter Schriftfarbe hervorgehoben. Der vorliegende Vertragstext gilt insofern als umfangreicherer Vertrag i. S. d. Klausel 2 Buchstabe b) des oben genannten Durchführungsbeschlusses sowie des vorliegenden Vertragsdokuments.

- Regelungen in grüner Texthervorhebungsfarbe zeigen eine Bearbeitungsnotwendigkeit an. Diese finden sich sowohl bei den Standardvertragsklauseln als auch bei den ergänzten Regelungen. **Alle Textstellen in grüner Texthervorhebungsfarbe sind zu bearbeiten**.

ANHANG
ABSCHNITT I

Klausel 1
Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln") soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)[1] sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2
Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3
Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4
Vorrang

[1] OPTION 2: Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG entfällt vorliegend mangels Einschlägigkeit.

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultativ
Kopplungsklausel
a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.
b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II
PFLICHTEN DER PARTEIEN

Klausel 6
Beschreibung der Verarbeitung
Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7
Pflichten der Parteien

7.1. Weisungen
a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung
Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten
Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung
a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von

beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.
d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens sechs Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der

Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

a. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung"), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679][2].

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679][3] in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679[4], die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn

[2] OPTION 2: Artikel 33 und Artikel 36 bis 38 der Verordnung (EU) 2018/1725] entfallen vorliegend mangels Einschlägigkeit.

[3] OPTION 2: Artikel 34 Absatz 3 der Verordnung (EU) 2018/1725 entfällt vorliegend mangels Einschlägigkeit.

[4] OPTION 2: Artikel 35 der Verordnung (EU) 2018/1725 entfällt vorliegend mangels Einschlägigkeit.

diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679[5] zu unterstützen.

ABSCHNITT III
SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

[5] OPTION 2: Artikel 34 und 35 der Verordnung (EU) 2018/1725 entfallen vorliegend mangels Einschlägigkeit.

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.
d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ABSCHNITT IV
ERGÄNZENDE VEREINBARUNGEN

Klausel 11
Konkretisierungen und ergänzende Regelungen

11.1 Pflichten der Parteien
a) Weisungen
Ergänzend zu Klausel 7.1 Buchstabe a) wird vereinbart:
Die Weisungen sind von den Vertragsparteien für die Geltungsdauer der Verarbeitung und anschließend noch für drei volle Kalenderjahre aufzubewahren.

b) Sicherheit der Verarbeitung
1) Ergänzend zu Klausel 7.4 Buchstabe a) wird vereinbart:

i) Die in Anhang III vereinbarten technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Bei allen Änderungen der technischen und organisatorischen Maßnahmen durch den Auftragsverarbeiter darf das Sicherheitsniveau der vereinbarten Maßnahmen nicht unterschritten werden.

ii) Bei Vergabeverfahren stellt der Auftragsverarbeiter dem Verantwortlichen bereits im Rahmen des Vergabeverfahrens zusammen mit seinem Angebot ein aussagekräftiges, prüffähiges und aktuelles Datenschutz- und Datensicherheitskonzept für diese Auftragsverarbeitung zur Verfügung.
Der Auftragsverarbeiter verarbeitet personenbezogene Daten (auch) in Mobiler Arbeit. Der Auftragsverarbeiter hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch bei „Mobiler Arbeiten" der Beschäftigten des Auftragsverarbeiters gewährleistet ist. Der Auftragsverarbeiter trägt Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten außerhalb der Geschäftsräume die Speicherorte so konfiguriert werden, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt. Der Auftragsverarbeiter trägt ferner dafür Sorge, dass die Bedingungen zum „Mobilen Arbeiten" des Auftragsverarbeiters einschließlich spezieller Verhaltens- und IT-

Sicherheitsrichtlinien, von den jeweiligen Beschäftigten eingehalten werden; die jeweiligen Beschäftigten werden hinsichtlich der Einhaltung datenschutzrechtlicher Anforderungen durch den Auftragsverarbeiter in geeigneter Weise geschult.

2) Ergänzend zu Klausel 7.4 Buchstabe b) wird vereinbart:
Die Pflicht zu Vertraulichkeit/Verschwiegenheit dieser Personen besteht auch nach Beendigung dieses Vertrages und/oder des Beschäftigungsverhältnisses zwischen dem Auftragsverarbeiter und den bei ihm Beschäftigten fort.

c) Dokumentation und Einhaltung der Klauseln
Ergänzend zu Klausel 7.6 Buchstabe a) wird vereinbart:
Der Auftragsverarbeiter unterstützt den Verantwortlichen auf dessen Verlangen bei der Erstellung und Führung des Verzeichnisses über die Verarbeitungstätigkeiten, insbesondere durch Mitteilung der erforderlichen Angaben.
d) Einsatz von Unterauftragsnehmern
Ergänzend zu Klausel 7.7 Buchstabe a) wird vereinbart:
Die Liste der bestehenden Unterauftragsverarbeiter wird dem Verantwortlichen vor Vertragsschluss zur Verfügung gestellt. Ergänzend zu Klausel 7.7 Buchstabe b) wird vereinbart:
Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

11.2 Unterstützung des Verantwortlichen
Ergänzend zu Klausel 8 Buchstabe a) wird vereinbart:
Der Auftragsverarbeiter darf Auskünfte an Dritte oder betroffene Personen nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen. Ist der Auftragsverarbeiter gerichtlich oder gesetzlich verpflichtet, Auskunft zu erteilen, so hat er den Verantwortlichen hierüber unverzüglich zu informieren. Der Auftragsverarbeiter darf Auskünfte an den Verantwortlichen nur gegenüber den autorisierten Personen (gemäß Anhang I) erteilen.
Ergänzend zu Klausel 10 Buchstabe d) wird vereinbart:
Ein Zurückbehaltungsrecht wird hinsichtlich der verarbeiteten personenbezogenen Daten und der zugehörigen Datenträger ausgeschlossen.

11.3 Meldung von Verletzungen des Schutzes personenbezogener Daten
Ergänzend zu Klausel 9 wird vereinbart:
Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich bei schwerwiegenden Störungen des Betriebsablaufs, Verdacht auf Verletzung des Schutzes personenbezogener Daten, anderen Unregelmäßigkeiten bei der Datenverarbeitung außerdem unverzüglich, bei Kontrollhandlungen und Maßnahmen einer Aufsichts- oder Ermittlungsbehörde. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn die bei ihm getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht (mehr) genügt.

Fernwartung

Fernwartung sind (zusätzlich) räumlich getrennte Zugriffe des Auftragsverarbeiters auf IT-Systeme des Verantwortlichen zu Wartungs- oder Reparaturzwecken.

a) Der Auftragsverarbeiter darf im Rahmen der Fernwartung nur auf personenbezogene Daten des Verantwortlichen zugreifen, wenn dies für die Durchführung der Fernwartung erforderlich ist. Ferner ist dem Auftragsverarbeiter bei der Fernwartung untersagt, personenbezogene Daten des Verantwortlichen auf eigenen IT-Systemen bzw. Datenträgern zu speichern, es sei denn der Verantwortliche weist ihn hierzu an. Der Verantwortliche wird dem Auftragsverarbeiter nur die für die Durchführung der vereinbarten Tätigkeiten benötigten Zugriffsrechte bereitstellen, deren Aktualität regelmäßig überprüfen und gegebenenfalls Korrekturen vornehmen. Der Auftragsverarbeiter darf von den ihm eingeräumten Zugriffsrechten nur in dem für die Durchführung der Tätigkeiten unerlässlichen Umfang Gebrauch machen.

b) Der Auftragsverarbeiter hat dem Verantwortlichen Fernwartungsarbeiten im Vorfeld anzukündigen. Der Verantwortliche ist berechtigt, die Durchführung der Fernwartung mit zu verfolgen bzw. Aufzeichnungen (z. B. Screenrecording, Screenshots o. Ä.) von dieser zu erstellen. Auf Anfrage und soweit erforderlich, wirkt der Auftragsverarbeiter an der Konfiguration technischer Kontrolleinrichtungen mit.

c) Der Verantwortliche hat das Recht, den Zugriff des Auftragsverarbeiters auf die informationstechnischen Systeme des Verantwortlichen zu unterbrechen. Dies gilt insbesondere, wenn der Verdacht besteht, dass unbefugt auf Informationen und Ressourcen zugegriffen wird.

d) Im Rahmen der beauftragten und zu leistenden Fernwartungsarbeiten hat der Auftragsverarbeiter folgende Rahmenbedingungen bei Zugriff auf das Netzwerk, die IT-Systeme und Anwendungen des Verantwortlichen zu beachten:

- Der Auftragsverarbeiter erhält für Arbeiten an den IT-Systemen und Anwendungen personalisierte Benutzerkennungen. Jeder Mitarbeiter des Auftragsverarbeiters erhält eine eigene personalisierte Benutzerkennung. Der Auftragsverarbeiter nutzt die ihm überlassenen personalisierten Benutzerkennungen ausschließlich für die beauftragten Tätigkeiten und gibt diese nicht an Dritte weiter. Die Kennwortrichtlinien des Verantwortlichen sind einzuhalten.
- Nutzt der Auftragsverarbeiter für die Ausübung seiner Tätigkeiten eigene technische Geräte stellt er durch adäquate und dem Stand der Technik entsprechende, angemessene Maßnahmen sicher, dass von diesen keine Gefahren für die Netzinfrastruktur, IT-Systeme und Anwendungen des Verantwortlichen ausgehen.
- Änderungen an den IT-Systemen und Anwendungen seitens des Auftragsverarbeiters sind mit dem Verantwortlichen abzustimmen und in einem adäquaten, prüffähigen Umfang zu dokumentieren.

11.5 Sonstiges

a) Die Haftung bemisst sich nach den Regelungen des Artikel 82 DS-GVO. Im Übrigen gelten für die Haftung die Regelungen des dieser Vereinbarung zugrundeliegenden Vertragsverhältnisses.

b) Änderungen, Ergänzungen und Nebenabreden dieses Vertrages sind schriftlich zu vereinbaren, was auch in einem elektronischen Format erfolgen kann.

c) Sollten in diesen Vereinbarungen eine oder mehrere Bestimmungen unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der übrigen Vertragsbestimmungen hierdurch nicht berührt. Die Vertragspartner werden die unwirksame oder undurchführbare Bestimmung durch eine Bestimmung ersetzen, die deren Sinn und Zweck am nächsten kommt. Gleiches gilt für den Fall einer ungewollten Regelungslücke.

Ort, Datum: ---------- Ort, Datum:----------

---------- ----------

Unterschrift Verantwortlicher Unterschrift Auftragsverarbeiter

ANHANG I

Liste der Parteien

Verantwortliche(r): [Name und Kontaktdaten des/der Verantwortlichen, und gegebenenfalls des Datenschutzbeauftragten des Verantwortlichen]
1. Name:
Anschrift:

Datenschutzbeauftragter: Jens Syckor, E-Mail: informationssicherheit@tu-dresen.de, Tel.: 0351 463 32839

Name, Funktion und Kontaktdaten der Kontaktperson:
.....
Weisungsberechtigt auf Seiten des Verantwortlichen ist:
>Name, Telefon, E-Mail, ggfs. Funktion, ggfs. Organisationseinheit<
Unterschrift und Beitrittsdatum: entfällt

Auftragsverarbeiter: [Name und Kontaktdaten des/der Auftragsverarbeiter/s und gegebenenfalls des Datenschutzbeauftragten des Auftragsverarbeiters]
1. Name:
Anschrift:

Weisungsempfänger auf Seiten des Auftragsverarbeiters ist:
> Name, Telefon, E-Mail, ggfs. Funktion, ggfs. Organisationseinheit<

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner*innen sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch Nachfolger*innen bzw. Vertreter*innen mitsamt Kontaktdaten mitzuteilen.

ANHANG II

Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden
☐ Studierende
☐ Studienbewerber*innen
☐ Beschäftigte
☐ Geschäftspartner*innen
☐ Proband*innen
☐ Sonstige Personen: .....

Kategorien personenbezogener Daten, die verarbeitet werden
.....
Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen
.....
Art der Verarbeitung
.....
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden
.....
Dauer der Verarbeitung
.....

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

Fernwartung
Bei Fernwartung werden die zusätzlich die unter 11.4 aufgenommenen Regelungen in Anlage III Bestandteil dieses Vertrages.
☐ **Ja**
☐ **Nein**

Drittlandtransfer

☐ Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt.
☐ Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet (ggf. zusätzlich zu einem Mitgliedsstaat der Europäischen Union) in dem /in den Folgenden genannten Drittland/Drittländern statt.

Das Datenschutzniveau im Drittland	☐ gemäß Klausel 7.8 Buchstabe b) dieses Vertrages **Abweichend, wie folgt**: ☐ ist festgestellt durch Angemessenheitsbeschluss der Kommission (Artikel 45 Absatz 3 DS-GVO), ☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artikel 46 Absatz 2 Buchstabe b) i.V.m 47 DS-GVO), ☐ wird hergestellt durch genehmigte Verhaltensregeln (Artikel 46 Absatz 2 e i.V.m. 40 DS-GVO), ☐ wird hergestellt durch ein Zertifizierungsmechanismus (Artikel 46 Absatz. 2 Buchstabe f) i.V.m. 42 DS-GVO), ☐ wird hergestellt durch sonstige Maßnahmen (Artikel 46 Absatz. 2 Buchstabe a), Absatz 3 Buchstabe a) und Buchstabe b) DS-GVO): **Welche**:_____

ANHANG III

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen angemessen dokumentiert werden.

*Beschreibung der von dem/den **Auftragsverarbeiter**[6] ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.*

Alternativ: *Der Auftragsverarbeiter hat dazu folgendes/folgende Dokument/e erstellt:*

_____

Die dort festgelegten technischen und organisatorischen Maßnahmen sind Bestandteil dieses Vertrages.

[6] Anpassung der Begrifflichkeit aufgrund eines augenscheinlichen Übersetzungsfehlers im Amtsblatt der Europäischen Kommission.

1. Vertraulichkeit

1.1. Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden.

☐ Es sind keine Maßnahmen zur Zutrittskontrolle erforderlich, weil .

☐ Es existieren keine Maßnahmen zur Zutrittskontrolle, weil .

☐ Es existieren folgende Maßnahmen zur Zutrittskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Alarmanlage	☐ Schlüsselregelung / Liste
☐ Automatisches Zugangskontrollsystem	☐ Empfang / Rezeption / Pförtner
☐ Biometrische Zugangssperren	☐ Besucherbuch / Protokoll der Besucher
☐ Chipkarten / Transpondersysteme	☐ Mitarbeiter- / Besucherausweise
☐ Manuelles Schließsystem	☐ Besucher in Begleitung durch Mitarbeiter
☐ Sicherheitsschlösser	☐ Sorgfalt bei Auswahl des Wachpersonals
☐ Schließsystem mit Codesperre	☐
☐ Absicherung der Gebäudeschächte	☐
☐ Türen mit Knauf Außenseite	☐
☐ Klingelanlage mit Kamera	☐
☐ Videoüberwachung der Eingänge	☐
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen sind .

1.2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen.

☐ Es sind keine Maßnahmen zur Zugangskontrolle erforderlich, weil .

☐ Es existieren keine Maßnahmen zur Zugangskontrolle, weil .

☐ Es existieren folgende Maßnahmen zur Zugangskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Login mit Benutzername + Passwort	☐ Verwalten von Benutzerberechtigungen
☐ Login mit biometrischen Daten	☐ Erstellen von Benutzerprofilen
☐ Anti-Viren-Software Server	☐ Zentrale Passwortvergabe
☐ Anti-Virus-Software Clients	☐ Richtlinie „Sicheres Passwort“
☐ Anti-Virus-Software mobile Geräte	☐ Richtlinie „Löschen / Vernichten“
☐ Firewall	☐ Richtlinie „Clean desk“

☐ Intrusion Detection Systeme	☐ Allg. Richtlinie Datenschutz und / oder Sicherheit
☐ Mobile Device Management	☐ Mobile Device Policy
☐ Einsatz VPN bei Remote-Zugriffen	☐ Anleitung „Manuelle Desktopsperre“
☐ Verschlüsselung von Datenträgern	☐
☐ Verschlüsselung Smartphones	☐
☐ Gehäuseverriegelung	☐
☐ BIOS Schutz (separates Passwort)	☐
☐ Sperre externer Schnittstellen (USB)	☐
☐ Automatische Desktopsperre	☐
☐ Verschlüsselung von Notebooks / Tablet	☐
☐	☐
☐	☐

Weitere Maßnahmen sind .

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können.

☐ Es sind keine Maßnahmen zur Zugriffskontrolle erforderlich, weil .

☐ Es existieren keine Maßnahmen zur Zugriffskontrolle, weil .

☐ Es existieren folgende Maßnahmen zur Zugriffskontrolle:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐ Aktenschredder (mind. Stufe 3, cross cut)	☐ Einsatz Berechtigungskonzepte
☐ Externer Aktenvernichter (DIN 32757)	☐ Minimale Anzahl an Administratoren
☐ Physische Löschung von Datenträgern	☐ Datenschutztresor
☐ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☐ Verwaltung Benutzerrechte durch Administratoren
☐	☐
☐	☐

Weitere Maßnahmen sind .

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

☐ Es sind keine Maßnahmen zur Trennungskontrolle erforderlich, weil .

☐ Es existieren keine Maßnahmen zur Trennungskontrolle, weil .

☐ Es existieren folgende Maßnahmen zur Trennungskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Trennung von Produktiv- und Testumgebung	☐ Steuerung über Berechtigungskonzept
☐ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☐ Festlegung von Datenbankrechten
☐ Mandantenfähigkeit relevanter Anwendungen	☐ Datensätze sind mit Zweckattributen versehen
☐	☐
☐	☐

Weitere Maßnahmen sind .

1.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

☐ Es sind keine Maßnahmen zur Pseudonymisierung erforderlich, weil .

☐ Es existieren keine Maßnahmen zur Pseudonymisierung, weil .

☐ Es existieren folgende Maßnahmen zur Pseudonymisierung:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	☐ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
☐	☐
☐	☐

Weitere Maßnahmen sind .

2. Integrität

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

☐ Es sind keine Maßnahmen zur Weitergabekontrolle erforderlich, weil .

☐ Es existieren keine Maßnahmen zur Weitergabekontrolle, weil .

☐ Es existieren folgende Maßnahmen zur Weitergabekontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Email-Verschlüsselung	☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☐ Einsatz von VPN	☐ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☐ Protokollierung der Zugriffe und Abrufe	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☐ Sichere Transportbehälter	☐ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☐ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☐ Persönliche Übergabe mit Protokoll
☐ Nutzung von Signaturverfahren	☐
☐	☐
☐	☐

Weitere Maßnahmen sind .

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind; ein Beispiel hierzu ist.

☐ Es sind keine Maßnahmen zur Eingabekontrolle erforderlich, weil .

☐ Es existieren keine Maßnahmen zur Eingabekontrolle, weil .

☐ Es existieren folgende Maßnahmen zur Eingabekontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☐ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☐ Manuelle oder automatisierte Kontrolle der Protokolle	☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
☐	☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐	☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden

☐	☐ Klare Zuständigkeiten für Löschungen

Weitere Maßnahmen sind .

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind: Beispiele sind insbesondere: Backup-Verfahren.

☐ Es sind keine Maßnahmen zur Verfügbarkeitskontrolle erforderlich, weil .

☐ Es existieren keine Maßnahmen zur Verfügbarkeitskontrolle, weil .

☐ Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐ Feuer- und Rauchmeldeanlagen	☐ Backup & Recovery-Konzept (ausformuliert)
☐ Feuerlöscher Serverraum	☐ Kontrolle des Sicherungsvorgangs
☐ Serverraumüberwachung Temperatur und Feuchtigkeit	☐ Regelmäßige Tests zur Datenwiederher-Herstellung und Protokollierung der Ergebnisse
☐ Serverraum klimatisiert	☐ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☐ USV	☐ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☐ Schutzsteckdosenleisten Serverraum	☐ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☐ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	☐ Getrennte Partitionen für Betriebssysteme und Daten
☐ RAID System / Festplattenspiegelung	☐
☐ Videoüberwachung Serverraum	☐
☐ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☐
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen sind .

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutzmanagement

☐ Es sind keine Maßnahmen zum Datenschutzmanagement erforderlich, weil .

☐ Es existieren keine Maßnahmen zum Datenschutzmanagement, weil .

☐ Es existieren folgende Maßnahmen zum Datenschutzmanagement:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Software-Lösungen für Datenschutzmanagement im Einsatz	☐ Interner / externer Datenschutzbeauftragter (siehe § 7)
☐ Zentrale Dokumentation aller Verfahrens weisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z. B. Wiki, Intranet)	☐ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
☐ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	☐ Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich
☐ Anderweitiges dokumentiertes Sicherheitskonzept	☐ Interner / externer Informationssicherheitsbeauftragter
☐ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☐ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
☐	☐ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
☐	☐ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
☐	☐
☐	☐

Weitere Maßnahmen sind .

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

☐ Es sind keine Maßnahmen zum Incident-Response-Management erforderlich, weil .

☐ Es existieren keine Maßnahmen zur Incident-Response-Management, weil .

☐ Es existieren folgende Maßnahmen zur Incident-Response-Management:

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Einsatz von Firewall und regelmäßige Aktualisierung	☐ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)

☐ Einsatz von Spamfilter und regelmäßige Aktualisierung	☐ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☐ Einsatz von Virenscanner und regelmäßige Aktualisierung	☐ Einbindung von DSB in Sicherheitsvorfälle und Datenpannen
☐ Intrusion Detection System (IDS)	☐ Dokumentation von Sicherheitsvorfällen und Datenpannen z. B. via Ticketsystem
☐ Intrusion Prevention System (IPS)	☐ Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen sind .

4.3. Datenschutzfreundliche Voreinstellungen

Privacy by Design / Default

☐ Es sind keine Maßnahmen zu datenschutzfreundlichen Voreinstellungen erforderlich, weil .

☐ Es existieren keine Maßnahmen zu datenschutzfreundlichen Voreinstellungen, weil .

☐ Es existieren folgende Maßnahmen zu datenschutzfreundlichen Voreinstellungen:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☐
☐ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	☐
☐	☐
☐	☐

Weitere Maßnahmen sind .

4.4. Auftragskontrolle (Outsourcing an Dritte)

Die weisungsgemäße Auftragsverarbeitung ist zu gewährleisten. Insbesondere sind hierbei die technischen und/oder organisatorischen Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer zu regeln.

☐ Es sind keine Maßnahmen zur Auftragskontrolle erforderlich, weil .

☐ Es existieren keine Maßnahmen zur Auftragskontrolle, weil .

☐ Es existieren folgende Maßnahmen zur Auftragskontrolle:

Technische Maßnahmen	Organisatorische Maßnahmen
☐	☐ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☐	☐ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
☐	☐ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
☐	☐ Schriftliche Weisungen an den Auftragnehmer
☐	☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☐	☐ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
☐	☐ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐	☐ Regelung zum Einsatz weiterer Subunternehmer
☐	☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐	☐ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Weitere Maßnahmen sind .